United Nations A/55/140

General Assembly

Distr.: General
10 July 2000
English
Original: Arabic/English/Russian

Fifty-fifth session
Item 69 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General**

Contents

		Page
I.	Introduction	2
II.	Replies received from Governments	2
	Jordan	2
	Qatar	3
	Russian Federation	3

* A/55/150.

** The present report is prepared on the basis of submissions from Member States.

00-53502 (E) 160800 210800

I. Introduction

1. The General Assembly, by paragraphs 2 and 3 of its resolution 54/49 of 1 December 1999 on developments in the field of information and telecommunications in the context of international security, invited all Member States to inform the Secretary-General of their views and assessments on the following questions: (a) general appreciation of the issues of information security, (b) definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources, and (c) advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality, and requested the Secretary-General to submit a report to it at its fifty-fifth session.

2. On 14 March 2000, the Secretary-General addressed a note verbale to Member States requesting them to provide their views pursuant to the invitation of the Assembly. The replies received to date from Governments are reproduced in chapter II of the present report. Any other replies received will be issued as addenda to the present report.

II. Replies received from Governments

Jordan

[Original: Arabic]
[16 May 1999]

1. The use of technology and information systems has had positive results for the international community in the maintenance of stability and security, but abuse of these new advances and techniques will:

(a) Make it easy to organize terrorist networks whose elements are dispersed over very extensive geographical areas, in view of the capabilities of rapid communications;

(b) Make it difficult to monitor modern communications in view of the rapidly evolving technological complexities and the existence in most countries of laws that limit interference in the freedom of individuals to communicate.

2. In our commitment to the adoption of appropriate measures, and as precautions against terrorist activity, we recommend the following:

(a) The formulation of a special emergency law to allow the security services to enter or partially control the control centres of companies handling advanced systems;

(b) Coordination with companies and establishments involved in communications to promote the training of specialists from the security services to handle such systems in times of crisis;

(c) Support for the information and communications technology sector and its related security concepts, and provision of infrastructure and appropriate training to promote the maintenance of international peace and security.

Qatar

[Original: Arabic]
[17 May 1999]

1. Espionage: preventing an unauthorized party from accessing the contents of global information and telecommunications systems.

2. Sabotage: preventing the partial or total destruction of global information and telecommunications systems.

3. Registration: registration of information sent through global information and telecommunications systems, including intellectual property.

4. Counterfeiting: preventing the counterfeiting of information sent through global information and telecommunications systems.

5. Protection: development of electronic protection for information sent through global information and telecommunications systems.

6. Legislation: formulation of the necessary laws for all electronic transactions in order to ensure the rights of participants and punish offenders.

Russian Federation

[Original: Russian]
[12 May 1999]

Principles of international information security

Use of terms

The following terms are used for the purposes of these Principles:

1. *Information area* — the sphere of activity involving the creation, transformation or use of information, including individual and social consciousness, the information and telecommunications infrastructure, and information itself.

2. *Information resources* — information infrastructure (hardware and systems for the creation, processing, storage and transmission of information), including bit maps, databases, information itself and data flows.

3. *Information war* — confrontation between States in the information area for the purpose of damaging information systems, processes and resources and vital structures, undermining political, economic and social systems as well as the massive psychological manipulation of a population in order to destabilize society and the State.

4. *Information weapons* — ways and means used for the purpose of damaging the information resources, processes and systems of a State, exerting an adverse influence, through information, on the defence, administrative, political, social, economic and other vital systems of a State, as well as the massive psychological manipulation of a population in order to destabilize society and the State.

5. *Information security* — a situation in which the basic interests of the individual, of society and of the State in the information area, including the information and telecommunications infrastructure and information itself with

respect to its characteristics such as integrity, objectivity, availability and confidentiality, are protected.

6. *Threat to information security* — factors that endanger the basic interests of the individual, of society and of the State in the information area.

7. *International information security* — a situation in international relations that precludes the violation of global stability and the creation of a threat to the security of States and of the world community in the information area.

8. *Illegal use of information and telecommunications systems and information resources* — the use of telecommunications and information systems and resources without the relevant entitlement or in violation of the established rules or legislation or the norms of international law.

9. *Unauthorized interference in information and telecommunications systems and information resources* — interference in the processes of the compilation, processing, accumulation, storage, presentation, retrieval, dissemination or use of information in order to disrupt the normal functioning of information systems or impair the integrity, confidentiality or accessibility of information resources.

10. *Vital structures* — facilities, systems and institutions of a State, deliberate influence on the information resources of which may have consequences that directly affect national security (transport, power supply, credit and financ communications, State administrative bodies, defence system, law enforcement agencies, strategic information resources, scientific facilities and scientific and technological developments, installations entailing a high degree of technological or ecological risk, bodies for the mitigation of the effects of natural disasters or other emergencies).

11. *International information terrorism* — the use of telecommunications and information systems and resources and exerting influence on such systems or resources in the international information area for terrorist purposes.

12. *International information crime* — the use of telecommunications and information systems and resources and exerting influence on such systems and resources in the international information area for illegal purposes.

Principle I

1. The activities of each State and of other subjects of international law in the international information area must be conducive to overall social and economic development and be conducted in a manner consistent with the objectives of maintaining global stability and security, and with the sovereign rights of other States, security interests, the principles of the peaceful settlement of disputes and conflicts, the non-use of force, non-interference in internal affairs and respect for human rights and freedoms.

2. Such activities must also be consistent with the right of everyone to seek, receive and disseminate information and ideas, as set forth in the relevant documents of the United Nations, bearing in mind that this right may be restricted by law in order to protect the security interests of each State.

3. At the same time, each State and other subjects of international law must have equal rights to protect their information resources and vital structures from illegal

use or from unauthorized interference in information, and shall be able to rely on the support of the world community in the attainment of those rights.

Principle II

States shall strive to restrict threats in the field of international information security and with that end in view shall refrain from:

(a) The development, creation and use of means of influencing or damaging another State's information resources and systems;

(b) The deliberate use of information to influence another State's vital structures;

(c) The use of information to undermine the political, economic and social system of other States, or to engage in the psychological manipulation of a population in order to destabilize society;

(d) Unauthorized interference in information and telecommunications systems and information resources, as well their unlawful use;

(e) Actions tending to establish domination or control in the information area;

(f) Preventing access to the most recent information technologies and the creation of conditions of technological dependency in the information field to the detriment of other States;

(g) Encouraging the activities of international terrorist, extremist or criminal associations, organizations, groups or individual law breakers that pose a threat to the information resources and vital structures of States;

(h) Formulating and adopting plans or doctrines envisaging the possibility of waging information wars and capable of instigating an arms race as well as causing tension in relations between States and specifically giving rise to information wars;

(i) The use of information technologies and tools to the detriment of fundamental human rights and freedoms in the field of information;

(j) The transboundary dissemination of information in contravention of the principles and norms of international law and of the domestic legislation of specific countries;

(k) The manipulation of information flows, disinformation and the concealment of information in order to corrupt the psychological and spiritual environment of society, and erode traditional cultural, moral, ethical and aesthetic values;

(l) Expansion in the field of information and the acquisition of control over the national information and telecommunications infrastructures of another State, including the conditions for their operation in the international information area.

Principle III

The United Nations and appropriate agencies of the United Nations system shall promote international cooperation for the purpose of limiting threats in the

field of international information security and creating, for that purpose, an international legal basis to:

(a) Identify the defining features of information wars and to classify them;

(b) Identify the characteristic features of information weapons, and of tools that may be regarded as information weapons, and to classify them;

(c) Restrict traffic in information weapons;

(d) Prohibit the development, dissemination or use of information weapons;

(e) Prevent the threat of the outbreak of information wars;

(f) Recognize the danger of using information weapons against vital structures as being comparable to the threat of use of weapons of mass destruction;

(g) Create conditions for the equitable and safe international exchange of information based on the generally recognized rules and principles of international law;

(h) Prevent the use of information technologies and tools for terrorist or other criminal purposes;

(i) Prevent the use of information technologies and tools to influence social consciousness in order to destabilize society and the State;

(j) Develop a procedure for the exchange of information on and the prevention of unauthorized transboundary influence through information;

(k) Create an international monitoring system for tracking threats that may arise in the information field;

(l) Create a mechanism for monitoring compliance with the conditions of the international information security regime;

(m) Create a mechanism to resolve conflict situations in the area of information security;

(n) Create an international system for the certification of information and telecommunications technologies and tools (including software and hardware) with a view to guaranteeing their information security;

(o) Develop a system of international cooperation among law enforcement agencies with a view to preventing and suppressing crime in the information area;

(p) Harmonize, on a voluntary basis, national legislation in order to ensure information security.

Principle IV

States and other subjects of international law must bear international responsibility for the activities in the information area that are carried out by them, whether under their jurisdiction or under the auspices of international organizations of which they are members, as well as for the conformity of any such activities with the principles set forth in this document.

Principle V

Any dispute between States or other subjects of international law that may arise from the application of these Principles shall be resolved through the use of the established procedures for the peaceful settlement of disputes.